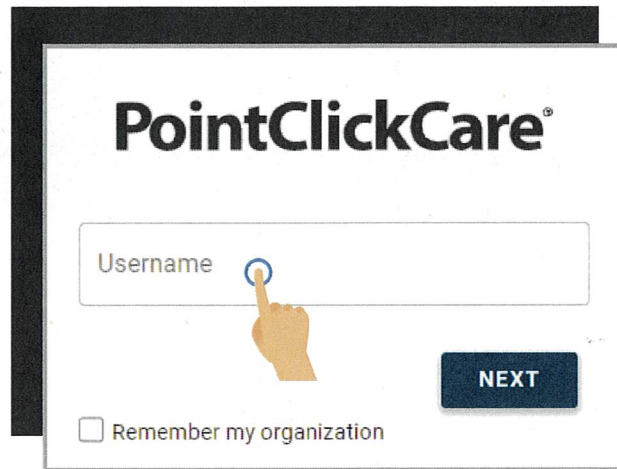
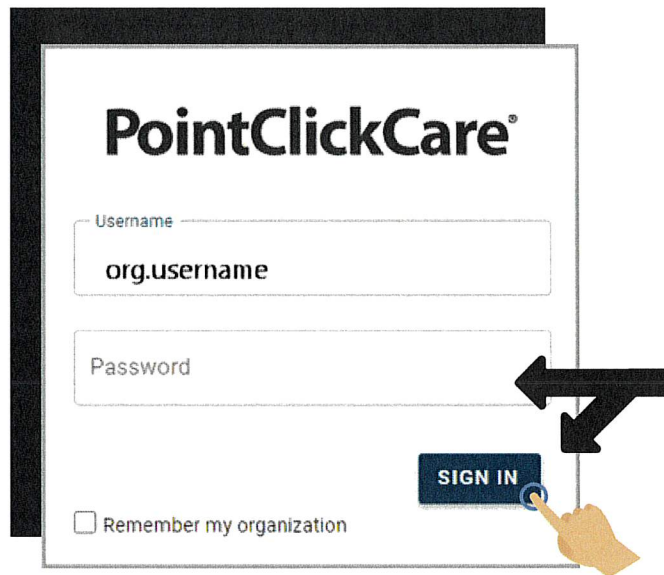


First Time Logging into PointClickCare using Multi-Factor Authentication

1. Navigate to the [PointClickCare Login Page](#).
2. Enter your **Username**.

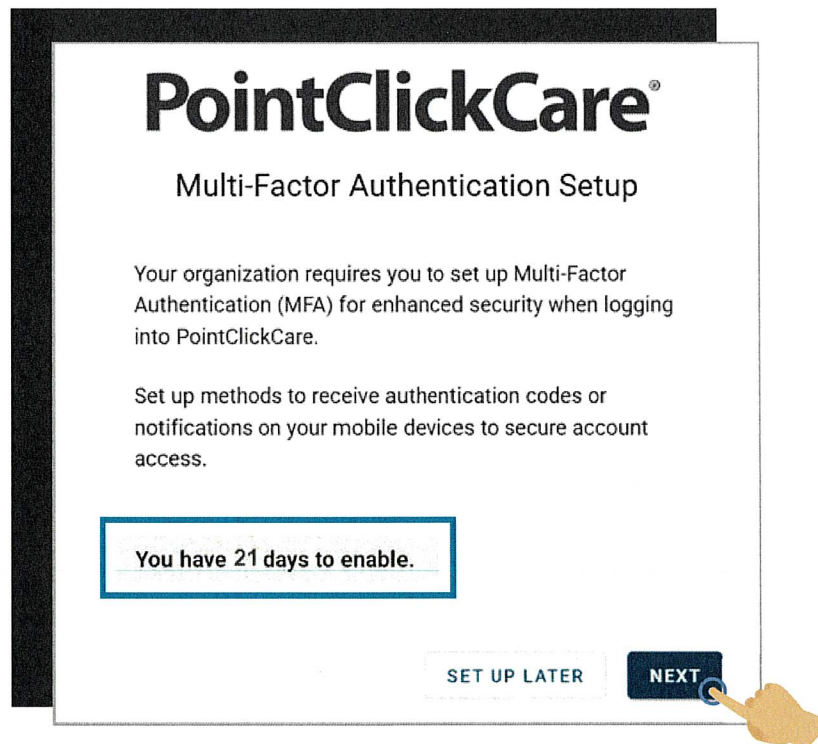
A screenshot of the PointClickCare login interface. At the top, the 'PointClickCare' logo is displayed. Below it is a text input field labeled 'Username'. A hand icon with a blue circle around the index finger is pointing at the input field. To the right of the input field is a dark blue button with the word 'NEXT' in white capital letters. Below the input field is a checkbox labeled 'Remember my organization'.

3. Enter your **Password** and select **SIGN IN**.



The image shows the PointClickCare login interface. At the top is the 'PointClickCare' logo. Below it are two input fields: 'Username' containing 'org.username' and 'Password'. A large black arrow points from the 'SIGN IN' button back to the 'Password' field. Below the password field is a checkbox labeled 'Remember my organization'. The 'SIGN IN' button is a dark blue rectangle with white text. A hand icon is shown clicking the 'SIGN IN' button.

4. Select **Next** on the Multi-Factor Authentication Setup Page.

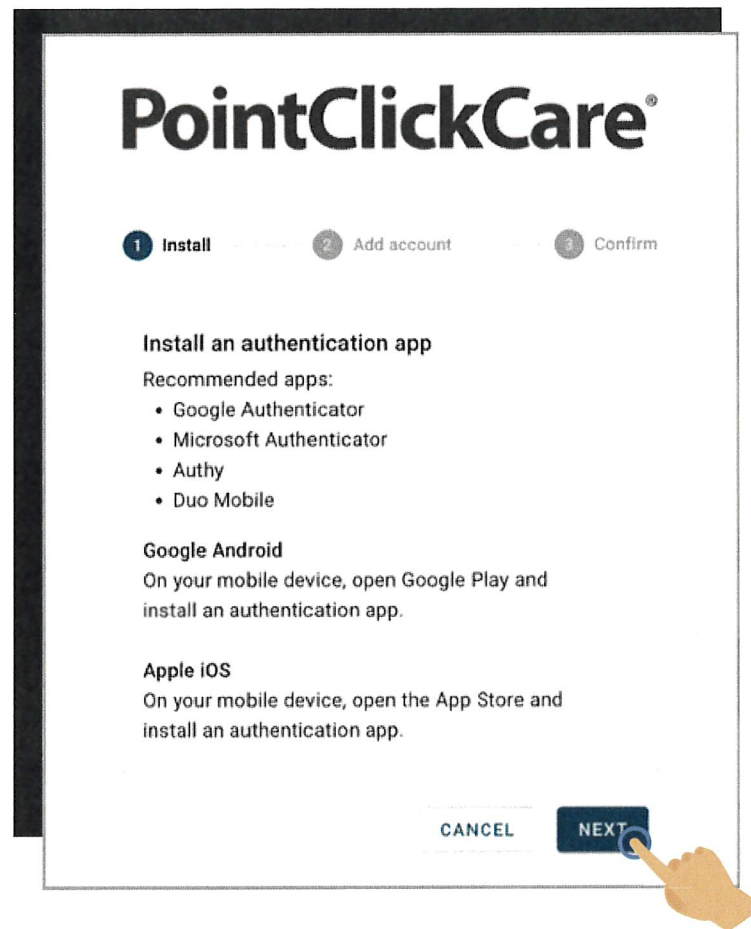


The image shows the 'Multi-Factor Authentication Setup' page. At the top is the 'PointClickCare' logo, followed by the title 'Multi-Factor Authentication Setup'. The main text reads: 'Your organization requires you to set up Multi-Factor Authentication (MFA) for enhanced security when logging into PointClickCare.' Below this is another line of text: 'Set up methods to receive authentication codes or notifications on your mobile devices to secure account access.' A blue-bordered box highlights the message: 'You have 21 days to enable.' At the bottom are two buttons: 'SET UP LATER' and 'NEXT'. A hand icon is shown clicking the 'NEXT' button.

If the allow MFA enrollment snooze for 21 days feature is activated in your community, you will see the highlighted message on your screen.

You are given the option to **SET UP LATER** or click **NEXT** to continue with the MFA Setup.

5. Ensure you have installed an Authentication app on your mobile device.
Select **NEXT**.



 **Note:** Download any Authenticator app from the **Apple Store or Google Play** on your mobile device. Below are some examples:

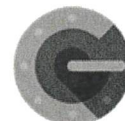
**Microsoft
Authenticator**



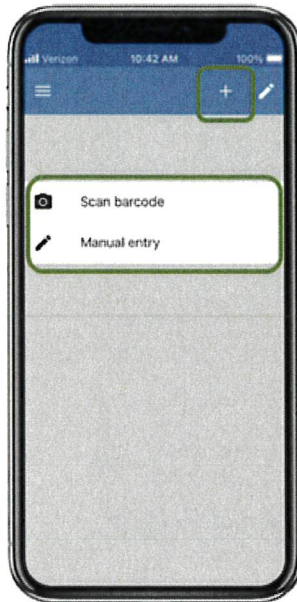
Authy



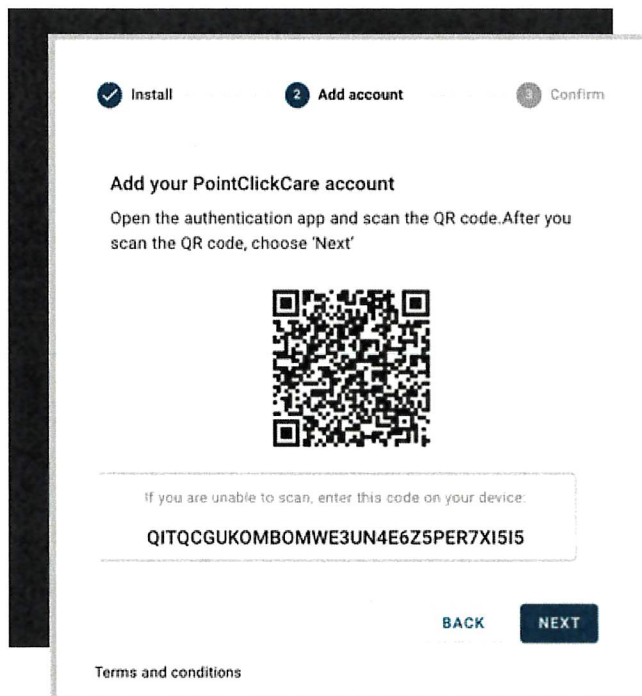
**Google
Authenticator**



6. On your mobile device, **open your Authenticator app** and select the option to add a new account. Select the **Scan QR Code** option.



7. **Scan the QR code** that's displayed on your computer into your Authenticator app (for mobile devices) or Sign in using the Code (for desktop Authenticator apps).



8. The Authenticator app is now connected to your account. The app **automatically starts generating time-based one-time passcodes**.



9. On your computer, enter the code generated by the Authenticator app in the verification code field.

Select **NEXT**.

✓ Install — ✓ Add account — 3 Confirm

Verify authentication

Enter the code generated by the authenticator.

1 [] [] [] [] []

Contact your System Administrator if you cannot access your authenticator app.

BACK NEXT

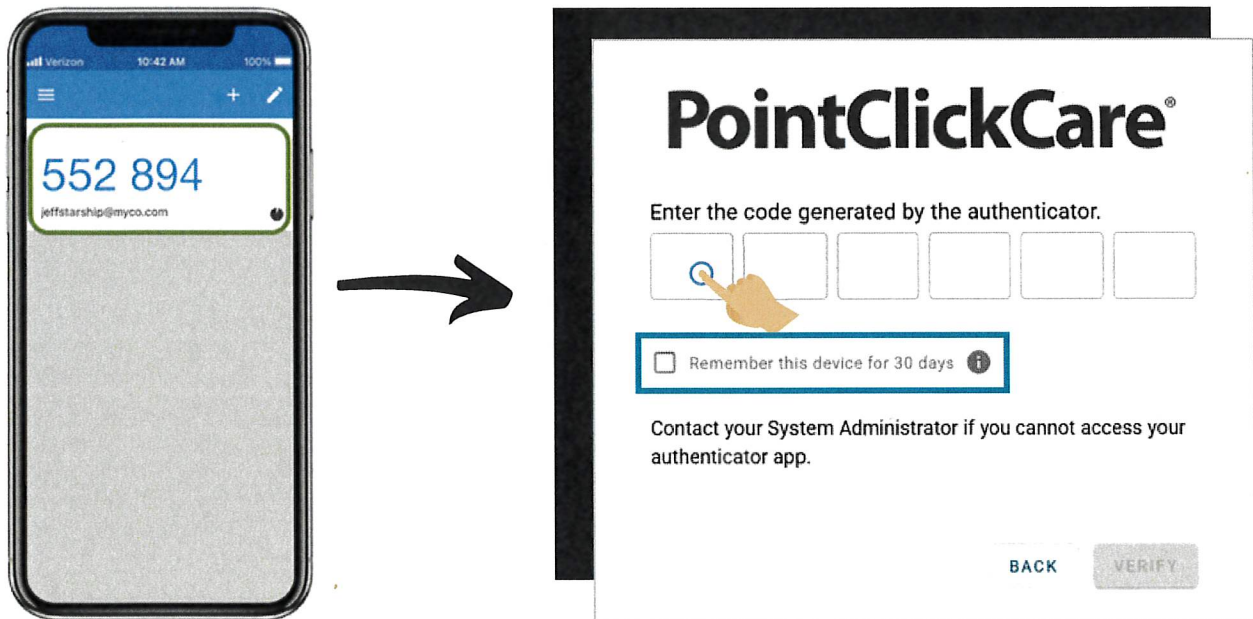
Terms and conditions



Note: Have you received an incorrect code error? Ensure your mobile device time is synced correctly.

Logging After Setting Up Multi-Factor Authentication

1. Navigate to the [PointClickCare Login Page](#).
2. Enter your **Username**.
3. Click **Next**.
4. Enter your **Password** and select **SIGN IN**.
5. To **verify authentication**, enter the code generated by your Authenticator app into the screen to log into PointClickCare.

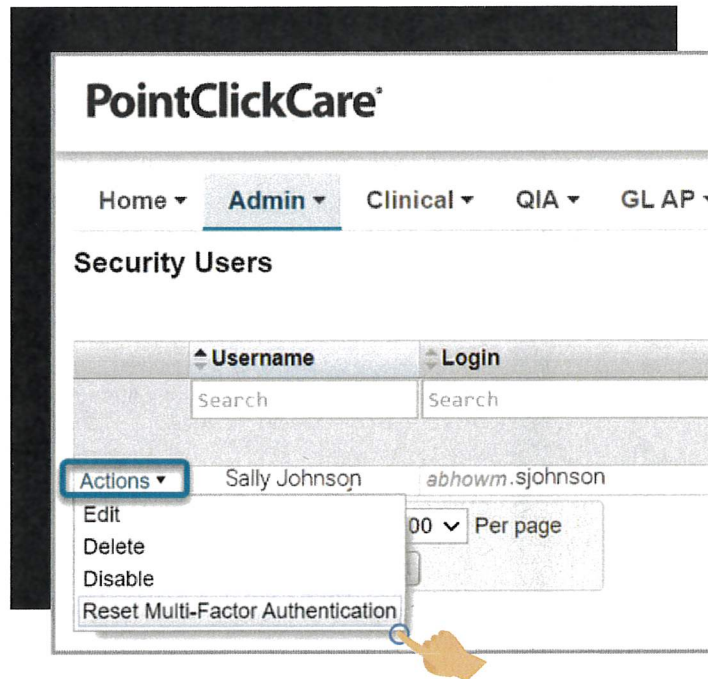


 **Note:** If your organization allows users to **skip MFA on trusted devices for 30 days**, you will see the highlighted message on your screen. Select the check box **before** entering the generated code.

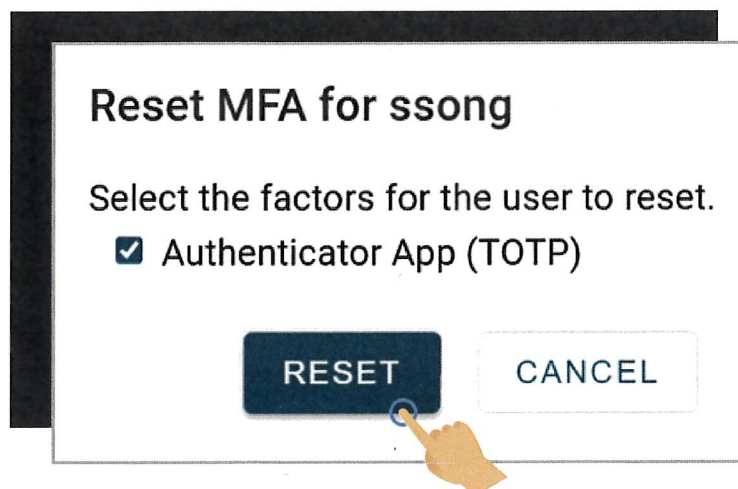
Once the code is entered, the screen will automatically change to the next step.

Reset Multi-Factor Authentication for a User

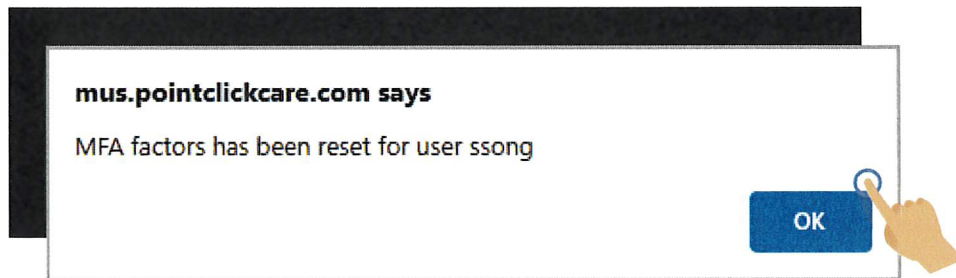
1. When a User requires Multi-Factor Authentication reset, navigate to **Security Users**.
2. Select **Actions** next to the User that requires reset.
3. Select **Reset Multi-Factor Authentication**.



4. Select the factors for the user to reset. Click **RESET**.



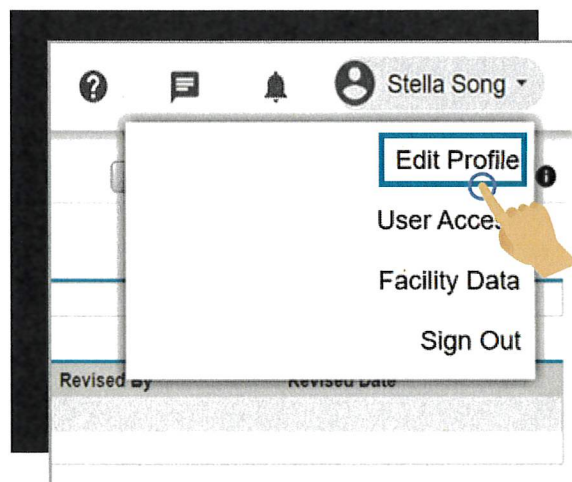
4. Click **OK**.



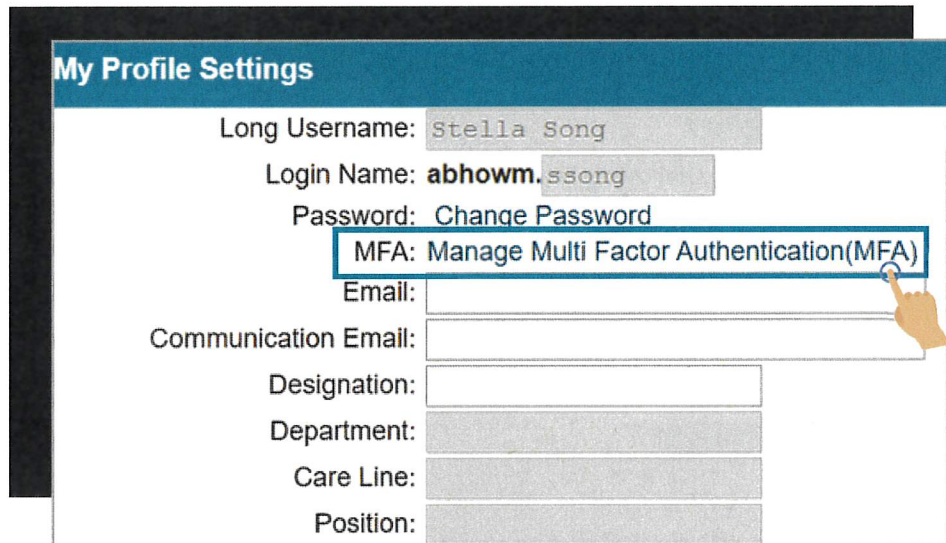
Manage Multi-Factor Authentication

As a user, you can enroll, reset, or manage MFA for your own account.

1. Click on your username and **Edit Profile**.



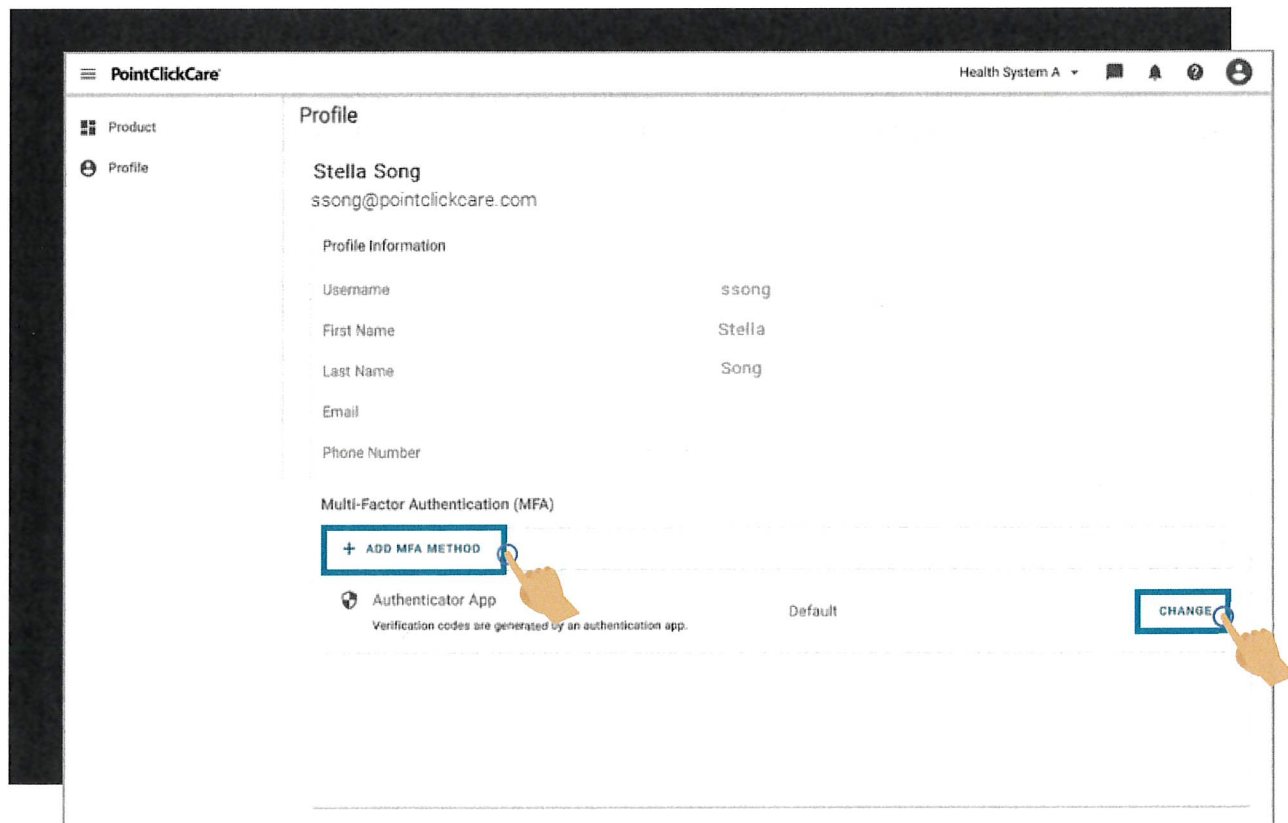
2. Click **Manage Multi Factor Authentication (MFA)**.



The screenshot shows a 'My Profile Settings' page. The 'MFA: Manage Multi Factor Authentication(MFA)' link is highlighted with a blue box and a hand icon pointing to it. Other fields include Long Username (Stella Song), Login Name (abhowm.ssong), Password (Change Password), Email, Communication Email, Designation, Department, Care Line, and Position.

3. Click **ADD MFA METHOD** to add a secondary method such as SMS.

4. Click **CHANGE** to select a different primary (default) MFA method.



The screenshot shows the PointClickCare Profile page for Stella Song (ssong@pointclickcare.com). Under the 'Multi-Factor Authentication (MFA)' section, the '+ ADD MFA METHOD' button is highlighted with a blue box and a hand icon. Below it, the 'Authenticator App' is listed as the 'Default' method, with a 'CHANGE' button highlighted with a blue box and a hand icon.